News Center
- Health Lawyers News
- Health Lawyers Weekly
  - **Archive**
  - Submissions to HLW
  - Subscribe to HLW
  - Editorial
  - Product Information
- Health Law Digest
- Health Law Documents
- Journal of Health Law
- Of Note
- Press Room

PRINT THIS PAGE
EMAIL A FRIEND

Health Information Technology

Editor's Note:

The following special feature is the text of the Key Note Speech delivered at the American Health Lawyers Association Masters Program on Health Information and Technology on April 6, 2006.

Implementing A Trusted Health Information Exchange

By Zoë Baird, President Markle Foundation

INTRODUCTION

Markle's Mission, Programs and Values

Advances in information technology (IT) continue to capture our imagination, promising a future with possibilities that go far beyond the revolutionary change we have already witnessed in business, finance and consumer choice. Technology, woven into the fabric of institutions that serve the public, can re-engineer how information is used to solve complex problems, meet critical public needs and empower people to improve their lives.

It is with an awareness of this transformative potential that the Markle Foundation has worked for the last few years to address critical public needs through the innovative use of information and IT and the creation of trusted information sharing environments.

The primary focus of the Markle Foundation is currently on two areas where we believe expanded use of IT and an improved exchange of information hold particular promise: the strengthening of our nation's security; and the modernization of our complex and over-burdened healthcare system. These are two of the most critical issues of our time, where the benefit to be gained from putting the right information in the right hands at the right time is enormous. In each of these areas, we know that the effective and appropriate use of IT can literally save lives. We also know that our nation's goals in both areas cannot be met without better use of IT.

At the same time, national security and healthcare also highlight a critical challenge we face in seeking new ways of using information: the need to protect our established values of privacy and civil liberties. Our commitment to designing new approaches to use and exchange information must always be coupled with the development of policy and technology solutions that protect privacy and civil liberties from the outset, not as an afterthought. It is our belief that if the policies and rules are not in place at the moment sensitive information, such as patient data, is shared, public trust will be undermined, and in the process the very viability of information-sharing will be threatened. In addition, we believe that these policies and business rules must be developed in a transparent, inclusive and accountable manner; only this will ensure that the public accepts—and, indeed, embraces—new uses of technology as legitimate and desirable.

So we recognize that using IT in new ways poses serious challenges. But we are equally aware of the tremendous opportunities. To meet these opportunities and complex challenges, the Markle Foundation engages with leaders and innovators

from technology, government, public interest organizations and business—from every sector of the healthcare and national security worlds.

In the National Security environment, we created the Task Force on National Security in the Information Age, a distinguished panel of security experts from five administrations, as well as experts on technology and civil liberties, which I am privileged to co-chair with Jim Barksdale, former CEO of Federal Express and Netscape.

Our most significant work in the health area has been Connecting for Health, a public-private collaborative comprised of an extraordinary group of government, industry, technology and healthcare leaders that has championed the national debate on electronic connectivity. It involves more than 100 organizations, including medical societies, technology vendors, insurance plans, government agencies, and consumer advocates, and is chaired by Carol Diamond, Managing Director of the Health Program at Markle.

In both areas, we work together to refine our vision and to bring about the technical and policy changes needed to enable breakthroughs in the public interest. This approach has allowed us to initiate large-scale, sustainable change, and to target issues where we believe a unique window of opportunity currently exists for positive transformation.

IMPLEMENTING A TRUSTED HEALTH INFORMATION EXCHANGE

I was asked by the organizers of this Masters Program to reflect on the policy and legal challenges in implementing a health information exchange. In doing so, I am building upon the lessons learned and solutions proposed by our Connecting for Health collaborative.

I am particularly delighted today to announce the launch of several papers and deliverables by Connecting for Health that aim to leverage the current window of opportunity in the healthcare area, and that suggest various ways to implement a private and secure health information exchange.

Context: U.S. Healthcare Today

But before getting into details, let me briefly reflect on the broader context of healthcare, and of health information technology in particular, so as to put the importance of our efforts into perspective:

Today, you can print a boarding pass from your home computer and get on an airplane. But when you go to a doctor's office, they hand you a clip board, pen and paper forms.

Today on the Internet you can compare the performance and prices of cars, personalize the car you want, and order and finance it from Detroit. But when you have a serious illness you don't have an electronic medical record of your health history; instead, you wind up carrying large files of paper and images around from doctor to hospital. No one is comparing or coordinating the wide array of professionals, technologies and medicines available to you; your care is delivered, and financed, in silos.

Consumers and doctors are dissatisfied with the quality and financing of today's healthcare system. Costs continue to escalate uncontrollably (premiums are up 25-30% in New York this year) while the quality of care received by too many patients is well below the standard that we are capable of achieving. Too many people die or suffer serious, often life-long, injuries from preventable medical errors.

National health expenditures were $1.7 trillion in 2003 and are projected to reach $3 trillion in 2012.[1] The United States continues to top the industrialized countries (OECD) ranking for overall healthcare spending at $5267 per capita—more than twice the OECD average of $2144.[2] Yet despite the much higher level of spending, various comparative studies have shown that:

- The United States does not rank higher on most quality of care measures

Seventh Circuit Fi
Relator Must Sho
That Was False

North Carolina To
Government $151
Medicaid Reimbu

Update

**Hospitals and I
Systems**

USC Seeks To Pa
Tenet Subsidiary

Medicaid

NASMD, APHSA
Not To Implement
Medicaid Regulat

Medicare

CMS Posts Medic
Data On Commor
Procedures

Eighth Circuit Say
Classroom Costs
Pass-Through Tre

Study Finds Varia
Plans' Drug Cove

News in Brief

CMS Solicits Prop
Risk Reduction D

compared to other countries;[3]

- Americans receive less hospital care, on average, than people in other industrialized countries, and see the doctor about as frequently.[4]

We have to change this!

The Disruptive Power of Information Technology

I believe that the best hope for change lies in the disruptive power of information technology to connect the fragmented parts of the U.S. Healthcare system and change the behavior of consumers and their doctors.

Health information and information technology (HIT) has the potential for dramatic improvements in quality of care and patient safety as well as efficiencies and cost savings. Computerized physician order entry and electronic medical records linked in a national network accessible by all healthcare organizations based on interoperable data standards can help bring real coordination to a fragmented healthcare system. Patients can also have easier access to their important health information, allowing them to be active participants in their own care.

Just imagine the man from Boston who has a heart attack on vacation in California; with IT, the emergency room could access his medical records electronically, discover he is allergic to aspirin, and avoid the serious, even fatal, medical error that would result from giving him this common treatment. Imagine the diabetic woman who could use home monitoring of her insulin levels and diet, shared electronically with her care providers, to efficiently make regular adjustments in her treatment and prevent complications. We are not just eliminating paperwork, but creating a new and stronger doctor-patient relationship, focused on better quality healthcare and greater efficiency.

Markle's Response: Connecting for Health and Its "Common Framework"

It is in large part to take advantage of opportunities like these that Markle, with additional funding and support from the Robert Wood Johnson Foundation, initiated and has operated the Connecting for Health program which I've already mentioned (*see* www.connectingforhealth.org).

Connecting for Health is committed to accelerating actions on a national basis that tackle the barriers that prevent us from applying the potential and power of IT to healthcare in the information age—and in doing so, to improve the quality of healthcare, reduce medical errors, lower costs, and empower patients.

Connecting for Health has been actively participating in shaping the national drive toward interoperable health. In its 2004 Roadmap document, "Achieving Electronic Connectivity in Healthcare: A Preliminary Roadmap from the Nation's Public and Private-Sector Healthcare Leaders," we recommended a common framework, comprising a set of immediate actions to be taken by all healthcare stakeholders to create a decentralized and standards-based information network.

Since then, attention to the need for information technology in healthcare has intensified, beginning with the President's call for the creation of electronic health records for all Americans, and encompassing numerous legislative bills, implementation of many government programs, the activities of the Office of the National Coordinator for Health Information Technology, and, last year, the establishment by Secretary Leavitt of the American Health Information Community (AHIC).

Based on the principles laid out in the Roadmap, Connecting for Health is now operating the first-ever prototype of an electronic national health information exchange based on common, open standards. This effort is the first step in enabling patients and authorized physicians in all 50 states and DC to share personal health information on a completely voluntary basis in a secure and private manner. The envisaged model, which includes the exchange of information both within and among local communities, is being conducted in California, Indiana, and Massachusetts, and has now been selected by the Office of the National Coordinator or ONCHIT along with three other contractors, as one approach for a prototype of a "Nationwide Health Information Network" (NHIN) architecture.

It is important to emphasize that prior to the launch of the prototype, Connecting for Health developed a series of core policy requirements and business rules to determine how technical architecture should enable improved exchange of information. More specifically, the group recommended that any prototype must do the following:

- guarantee that patients and their authorized health professionals jointly make decisions regarding the sharing of health information, a step that will increase the public trust that is necessary from the outset (I will discuss this point in greater detail later);
- facilitate communication among numerous, disparate information networks and diverse communities in a federated, decentralized manner;
- build upon the existing Internet infrastructure while allowing for diversity in software and hardware;
- identify areas that *require* national uniformity—to permit broad exchange of information—while also enabling customization to regional and local preference and legacy infrastructure.

The Launch of "Resources for Implementing Private and Secure Health Information Exchange"

Early on, it became clear that a sustainable environment for exchanging health information required technological design decisions to be developed in sync with policies and business rules that fostered trust and transparency.

Towards that end, Connecting for Health and its working groups have focused on the development of a "common policy and technology framework," in the form of a set of resources that government, communities and other networks can use to leverage their existing IT investments for better information sharing while protecting privacy and security.

Today we are releasing the first bundle of such resources—including privacy policies, technical network specifications, and model contracts—that we believe will enable this kind of trusted information sharing, and put in place an infrastructure to support health system improvement.

It suggests practical solutions to a whole set of challenges that were not anticipated in past legislative or professional assessments, while sustaining the values of the American public.

Our approach can be thought of as working from "principles to policies to practice." First, we have tried to articulate and achieve broad consensus on essential principles that govern the handling of sensitive health information. Second, we have tried to express those principles into explicit and formal policy statements. And third, we encourage practitioners—attorneys, industry leaders, technologists, community leaders—to implement systems on the ground that apply and enforce those policies.

This explains why I am delighted to present some of our findings to you. As lawyers in the field, you are indispensable to shaping, educating, and achieving that most vital final translation, from policies and rules, to actual practice. While we can draft guidelines, it is up to practitioners like you to ensure that they are actually implemented—and, in doing so, to ensure that privacy and civil liberties are strengthened with enhanced information-sharing.

Focus on Privacy

Let me explain our approach further by focusing on a specific area that may be of particular relevance for the Masters Program—namely, the need to protect the privacy of medical records in a connected and networked environment.

As indicated earlier, we have to address the privacy and security issues up front or the business models that will drive the adoption of health and information technology will not be sustainable. Just look at the reaction against the architecture of cookies, which allow companies to share information about consumers without their consent; a popular backlash has led to consumers installing anti-spy ware and other tools to block such cookies.

Perhaps more importantly, a lack of trust in how medical data is gathered, used and disclosed is ultimately harmful to patients because it can lead to so-called “privacy protective behavior.” Such behavior includes hiding evidence of pre-existing conditions from doctors or insurance companies; paying out-of-pocket for treatment; or simply avoiding treatment altogether. A lack of trust has a toll on both individual health and, more generally, on public health.

These concerns with regard to the increased privacy risks posed by technology among the public are real and increasing.

Recent high profile cases of security and data breaches—many of which have been reported in the media—have dramatically highlighted the inherent vulnerabilities of networks and information stored in a digital form. From January 1 to November 1, 2005, there were 118 known security breaches, which impacted potentially 57 million individuals. So far, many of the breaches have affected financial information, but at least 10 of the breaches have been specifically related to medical information. At the same time, identity theft has become a major consumer concern. According to a recent poll, 20% of American adults, or 44 million individuals, reported in 2005 that their identity has been stolen as result of data leakage or theft.

These breaches and thefts have substantially increased already existing concerns regarding health privacy. These concerns have been documented by a number of recent surveys:

- A Harris Interactive Survey on Medical Privacy, released on F*ebruary 8, 2005, indicated that* between 62% and 70% of adults are worried that sensitive health information might leak because of weak data security; that there could be more sharing of patients' medical information without their knowledge; that computerization could increase rather than decrease medical errors; that some people won't disclose necessary information to healthcare providers because of worries that it will be stored in computerized records; and that existing federal health privacy rules will be reduced in the name of efficiency.
- A California Health Care Foundation survey (November 2005) indicated that 67% of Americans remain concerned about the privacy of their personal health information and are largely unaware of their rights;
- A Markle Foundation survey, released in October 2005, found that more than three out of four respondents (79%) supported the right of a patient to control access to personal health information.

It is essential to realize that these increased risks, and the growing distrust among the public, cannot sufficiently be dealt with through existing legal provisions such as HIPAA and subsequent privacy practices which were developed well before the advent of networked, portable health information systems. These new risks require comprehensive “architectural” solutions that build privacy and security protections from the start, rather than as post-fact remedies.

As I mentioned, one model for such a comprehensive privacy architecture has been developed by Connecting for Health. The “Connecting for Health Architecture for Privacy in a Networked Health Environment” recommends nine privacy protection principles, building upon existing fair information practices adopted in various countries. Considered and applied together, these principles add up to an integrated and comprehensive approach to privacy that can help overcome the current fragmentation of American healthcare.

In the remainder of this speech, I’m going to discuss these nine principles.

The first principle is that of **Openness**. It holds that there should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, the main purposes of their use, as well as the identity and usual residence of the data controller.

The second principle is that of **Purpose Specification and Minimization**. It holds that the purpose for which personal data are collected should be specified not later than at the time of data collection, and the subsequent use should be limited to those purposes or others that are compatible or that are specified on each occasion of change of purpose.

A third principle is that of **Collection Limitation**. According to this principle, there should be limits to the collection of personal data. Any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Fourth, Connecting for Health upholds a principle of **Use Limitation**. This means that personal data should not be disclosed, made available or otherwise used, except with the consent of the data subject or by the authority of law.

The fifth principle is that of **Individual Participation and Control**. It holds that an individual should have the right to know, and the means to find out (e.g., through a written request) how his or her data are being used. In addition, individuals should also have the right to challenge how their data are being used. In the healthcare context, this principle is controversial and is likely to take up much of your time in the coming years. Can a patient—or caregiver—determine whether his or her information is to be shared? And whether specific information may be shared with various individuals? Will our new information technologies permit this kind of control? And how will doctors and managers view increased patient management of the data they need to do their jobs?

The sixth principle is that of **Data Integrity and Quality**. It holds that personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Seventh, personal data should be protected by ***reasonable security safeguards*** against risks such as loss or unauthorized access, destruction, use, modification or disclosure of data.

The eight principle calls for **Accountability and Oversight**. It states that a data controller should be accountable for complying with measures, which give effect to the other principles. Compliance with all of these basic principles is especially important for a system which will contain and disseminate highly personal information of the utmost sensitivity.

Finally, the ninth architectural principle proposed by Connecting for Health draws attention to the need for **Remedies**. It holds that legal and financial remedies must exist to address any security breaches or privacy violations.

Of course, the principles remain just that—principles—and their precise manifestation will vary from state to state, and from application to application. Yet while they are broad enough to apply across organizations, stakeholders, and jurisdictions, they are also specific and tangible enough to have real significance and practical effect. The key is to apply them in a thorough and comprehensive manner before creating any new health information network, not as an afterthought, and not as an after-the-fact band-aid solution.

To achieve this, we must turn them into operating policies for use at the community or network level. Towards that end, Connecting for Health has convened several committees, comprised of dozens of national leaders—attorneys, ethicists, consumer advocates, medical associations, health plans, and so on—to identify those issues which required formal policy development and to seek consensus on the relevant policies. These committees worked for over a year. The policy papers included in the CD we release today provide the first steps in translating our principles into policies. I won't attempt to summarize them here, but only advise you that our collaborative has for instance addressed identity management policies, data accuracy issues, and procedures for patient's consent and control of information. In addition, to help communities and networks make the transition from these core principles and policies to the very concrete realities of business and practice, we've developed a model contract that identifies those issues needing national uniformity and those that need regional or network-based agreement.

And here, of course, is where we so urgently need your help—and that of your colleagues throughout the nation. You represent the most experienced and expert attorneys in the area of health IT in our country, and it will be to you that others will turn for advice and leadership on the great challenges that face us: to improve healthcare through freer information exchange, while also continuing to protect individuals' privacy and confidence in the system. Our hope is that you will review these documents, evaluate them, criticize them, add to them, and use them. We'd like

you to both make them your own—and tell us how they must be improved.

As I said earlier, we believe that a core set of policies must provide a uniform foundation for nationwide information sharing—that much can be left to local discretion, but that some critical elements must be accepted and enforced on a national basis. Please help us refine our understanding of where that boundary is, always seeking to minimize the imposed national requirements while preserving the trustworthiness and efficiency of the overall system.

CONCLUSION

Today's Master's Class takes place at a unique moment in time. The President, HHS, the National Health Information Technology Coordinator, and literally thousands of other actors are currently considering nationally, regionally and locally how to share health information using information technology.

Lawyers like you are essential to understanding the issues at stake—to integrate and fine-tune comprehensive response to the numerous policy challenges we face. I hope the material we launch today will be elaborated and developed in greater detail with your input. I look forward to discussing the many possibilities for working together on these important issues.

---

[1] See *CMS: National Healthcare Expenditures Projections,* available at *http://www.cms.hhs.gov/statistics/nhe/historical/highlights.asp* and *CMS: Health Spending Projections Through 2013*, By Stephen Heffler, Sheila Smith, Sean Keehan, M. Kent Clemens, Mark Zezza, and Christopher Truffer, In: *Health Affairs*, (February 11, 2004), available at http://content.healthaffairs.org/cgi/content/full/hlthaff.w4.79v1/DC1.

[2] See *Health Spending in Most OECD Countries Rises, with the U.S. far Outstripping all Others*. By: Organisation for Economic Co-operation and Development (March 6, 2004), available at: http://www.oecd.org/document/12/0,2340,en_2649_37407_31938380_119656_1_1_37407,00.html.

[3] See *Common Concerns Amid Diverse Systems: Healthcare Experiences In Five Countries*. By Robert Blendon et al., In: *Health Affairs* (May/June 2003).

[4] See *Multinational Comparisons of Health Systems Data, 2002*. By Anderson et al., *bb*, (October 2002).